CLAIMS

What is claimed is:

1. A method for authenticating messages communicated between partners that belong to a plurality of partners, the method comprising the steps of:

maintaining at a trusted intermediary a signature decryption key for each partner of said plurality of partners that is authorized to use said trusted intermediary to send messages;

receiving at said trusted intermediary messages originated by partners of said plurality of partners that are intended for other partners of said plurality of partners;

for each message thus received, the trusted intermediary performing the steps of

using the signature decryption key associated with the partner that sent the message to determine whether the message was actually sent by that partner; and

if the message was actually sent by that partner, then sending the message to the partner for which the message is intended along with a digital signature of said trusted intermediary to indicate that the trusted intermediary has verified that the message was actually sent by the partner that sent the message.

2. The method of Claim 1 wherein the signature decryption key for each partner of said plurality of partners is a public signature decryption key associated with a private signature creation key.

3. The method of Claim 1 wherein the signature decryption key for each partner of said plurality of partner is used to decrypt a digital signature associated with a message that is sent along with the digital signature.

4. The method of Claim 1 wherein the digital signature of the trusted intermediary is associated with a message that is sent along the digital signature of the trusted intermediary.

5. The method of Claim 1 wherein the digital signature of the trusted intermediary is encrypted by a private signature creation key associated with a public signature decryption key.

6. A computer-readable medium storing computer code for causing a computer to perform a method for authenticating messages communicated between partners that belong to a plurality of partners, by the steps of:

maintaining at a trusted intermediary a signature decryption key for each partner of said plurality of partners;

receiving at said trusted intermediary messages originated by partners of said plurality of partners that are intended for other partners of said plurality of partners;

for each message thus received, the trusted intermediary performing the steps of

using the signature decryption key associated with the partner that sent the message to determine whether the message was actually sent by that partner; and

if the message was actually sent by that partner, then sending the message to the partner for which the message is intended along with a digital signature of said trusted intermediary to indicate that the trusted intermediary has verified that the message was sent actually sent by the partner that sent the message.

7. The computer-readable medium of Claim 6 wherein the signature decryption key for each partner is a public signature decryption key associated with a private signature creation key.

8. The computer-readable medium of Claim 6 wherein the signature decryption key for each partner is used to decrypt a digital signature associated with a message is that sent along with the digital signature.

9. The computer-readable medium of Claim 6 wherein the digital signature of the trusted intermediary is associated with a message that is sent along with the digital signature.

10. The computer-readable medium of Claim 6 wherein the digital signature of the trusted intermediary is encrypted by a private signature creation key associated with a public signature decryption key.

11. A computer for use in communications between partners that belong to a plurality of partners, comprising:

storage means configured to store a signature decryption key for each partner of said plurality of partners that is authorized to use said computer to send messages;

receiving means configured to receive messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of partners;

signature decryption means; and

sending means; wherein

for each message thus received,

said signature decryption means is configured to use the signature decryption key associated with the partner that sent the message to determine whether the message was actually sent by that partner; and

if the message was actually sent by that partner, said sending means is configured to send the message along with a digital signature of said trusted intermediary to the partner for which the message is intended; wherein said digital signature of said trusted intermediary is used to indicate that said trusted intermediary has verified that the message was actually sent by the partner that sent the message.

12. The computer of claim 11 further comprising signature encryption means by which said digital signature of said trusted intermediary was created.

13. A computer network for use in communications between partners that belong to a plurality of partners, comprising:

a plurality of computers each of which is configured to store a respective signature creation key of a partner of said plurality of partners that is authorized to use a trusted intermediary computer to send messages;

wherein said trusted intermediary computer is configured

to store a plurality of signature decryption keys each of which corresponds to the respective signature creation key that is stored in each of said plurality of computers;

wherein, upon receiving messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of partners, said trusted intermediary computer, for each message thus received, is configured

to use the signature decryption key associated with the partner that sent the message to determine whether the message was actually sent by that partner; and

if the message was actually sent by that partner, then sending the message to the partner for which the message is intended along with a digital signature of said trusted intermediary to indicate that the trusted intermediary

has verified that the message was actually sent by that partner that sent the message.

14. A method for a trusted intermediary to manage keys used in communications between partners that belong to a plurality of partners, the method comprising the steps of:

a trusted intermediary maintaining a message encryption key for each partner of said plurality of partners that is authorized to use said trusted intermediary to receive messages; wherein

upon receiving messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of partners, said trusted intermediary, for each message thus received, performing the steps of

encrypting the message using the message encryption key associated with the partner for which the message is intended; and

sending the encrypted message to the partner for which the message is intended.

15. The method of Claim 14 wherein the message encryption key for each partner of said plurality of partners is a public message encryption key associated with a private message decryption key.

16. The method of Claim 14 wherein each of the messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of

partners was encrypted using a message encryption key associated with the trusted intermediary.

17. The method of Claim 16 wherein said message encryption key associated with said trusted intermediary is a public message encryption key that is associated with a private message decryption key.

18. A computer-readable medium storing computer code for causing a computer to perform a method for a trusted intermediary to manage keys used in communications between partners that belong to a plurality of partners, by the steps of:

said trusted intermediary maintaining a message encryption key for each partner of said plurality of partners that is authorized to use said trusted intermediary to receive messages; wherein

upon receiving messages originated by partners of said plurality of partners that are intended for other partners of said plurality of partners, said trusted intermediary, for each message thus received, performing the steps of

encrypting the message using the message encryption key associated with the partner for which the message is intended; and

sending the encrypted message to the partner for which the message is intended.

19. The computer-readable medium of Claim 18 wherein the message encryption key for each partner of said plurality of partners is a public message encryption key associated with a private message decryption key.

20. The computer-readable medium of Claim 18 wherein the computer further performs the step of:

each partner of said plurality of partners that sends messages to said trusted intermediary maintains a message encryption key associated with a message decryption key of said trusted intermediary.

21. The computer-readable medium of Claim 20 wherein said message encryption key associated with said message decryption key of said trusted intermediary is a public message encryption key and said message decryption key of said trusted intermediary is a private message decryption key.

22. A computer for use in communications between partners that belong to a plurality of partners, comprising:

storage means configured to store a message encryption key for each partner of said plurality of partners that is authorized to use said computer to receive messages;

message encryption means;

sending means; and

receiving means configured to receive messages that are originated by partners of said plurality of partners and that are intended for other partners of said plurality of partners; wherein

for each message thus received,

said message encryption means encrypts the message using the message encryption key associated with the partner for which the message is intended; and

said sending means sends the encrypted message to the partner for which the message is intended.

23. The computer system of claim 22 further comprising message decryption means that, for each message thus received, produces that message from an encrypted message.

24. A computer network for use in communications between partners that belong to a plurality of partners, comprising:

a plurality of computers each of which is configured to store a respective message decryption key of a partner of said plurality of partners that is authorized to use a trusted intermediary computer to receive messages;

wherein said trusted intermediary computer is configured

to store a plurality of message encryption keys each of which corresponds to the respective message decryption key that is stored in each of said plurality of computers;

wherein, upon receiving messages that are originated by partners of said plurality of partners and that are intended for others partners of said

plurality of partners, said trusted intermediary computer, for each message thus received, is configured

to encrypt the message using the message encryption key associated with the partner for which the message is intended, and

to send the encrypted message to the partner for which the message is intended.